UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/725,208	12/02/2003	Masato Yamamichi	2003_1741A	4485

52349 7590 01/19/2007
WENDEROTH, LIND & PONACK L.L.P.
2033 K. STREET, NW
SUITE 800
WASHINGTON, DC 20006

EXAMINER	
LOUIE, OSCAR A	
ART UNIT	PAPER NUMBER
2112	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/19/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/725,208	YAMAMICHI ET AL.	
	Examiner	Art Unit	
	Oscar A. Louie	2112	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 December 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-43* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-43* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *04 May 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *02/05; 05/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This first non-final action is in response to the original filing of 12/02/2003. Claims 1-43 are pending and have been considered as follows.

Double Patenting

1. Claims 1-7, 9-33, 37-40, & 43 of this application conflict with claims 1-12, 14-32, & 36-51 of Application No. 10/725102. 37 CFR 1.78(b) provides that when two or more applications filed by the same applicant contain conflicting claims, elimination of such claims from all but one application may be required in the absence of good and sufficient reason for their retention during pendency in more than one application. Applicant is required to either cancel the conflicting claims from all but one application or maintain a clear line of demarcation between the applications. See MPEP § 822.

Claim 1:

- Claim 1 of Application No. 10/725208 discloses a key agreement system comprising equivalent elements as Claim 1 of Application No. 10/725102. The features disclosed as two elements in Claim 1 of Application No. 10/725208 as, "a first encryption unit," and, "second encryption unit," are equivalent to, "an encryption unit," which is disclosed as a single element by Claim 1 of Application No. 10/725102.

Claim 2:

- Claim 2 of Application No. 10/725208 discloses equivalent elements to Claim 2 of Application No. 10/725102.

Claim 3:

- Claim 3 of Application No. 10/725102 discloses a shared-key generation apparatus for use in the system as in Claim 1 above, and comprises of equivalent elements as Claim 3 of Application No. 10/725208. The features disclosed as two elements in Claim 3 of Application No. 10/725102 as, "a first encryption unit," and, "second encryption unit," are equivalent to, "an encryption unit," which is disclosed as a single element by Claim 3 of Application No. 10/725208.

Claim 4:

- Claim 4 of Application No. 10/725102 and Claim 16 of Application No. 10/725208, disclose equivalent elements.

Claim 5:

- Claim 5 of Application No. 10/725102 and Claims 7 & 17 of Application No. 10/725208, disclose equivalent elements. Claim 4 of Application No. 10/725208 discloses, "the shared-key generating unit performs a one-way function on the seed value, to generate the functional value, and generates the blind value and the shared key from the functional value," which is equivalent to Claim 5 of Application No. 10/725102.

Claims 6, 18, 32, & 38:

- Claims 6, 18, 32, & 38 of Application No. 10/725102 and Claims 8 & 18 of Application No. 10/725208, disclose equivalent elements.

Claims 7 & 39:

- Claim 19 of Application No. 10/725208 discloses elements equivalent to Claims 7 & 39 of Application No. 10/725102.

Claim 8:

- Claim 8 of Application No. 10/725102 and Claim 17 of Application No. 10/725208, disclose equivalent elements. Claim 10 of Application No. 10/725208 discloses, "the shared-key generating unit performs a one-way function on the seed value, to generate a functional value, and generates a verification value, the blind value, and the shared key," which is equivalent to Claim 8 of Application No. 10/725102.

Claims 9 & 11:

- Claims 4, 6, & 10 of Application No. 10/725208 disclose, "a public-key obtaining subunit operable to obtain a public key; and a public-key encryption subunit operable to perform a public-key encryption algorithm on the seed value, using the public key and the blind value, to generate an encryption seed value as the encryption information," and, a public-key obtaining subunit operable to obtain a public key; a public-key encryption subunit operable to generate a blind value, perform the public-key encryption algorithm on the seed value using the public key and the blind value, to generate a public-key cipher text," and, "a public-key obtaining subunit operable to obtain a public key; a first encryption subunit operable to perform a public-key encryption algorithm on the verification value, using the public key and the blind value, to generate a first cipher text," which is equivalent to Claims 9 & 11 of Application No. 10/725102.

Claims 10 & 12:

- Claims 5, 9, & 11 of Application No. 10/725208 disclose, "the public-key encryption algorithm conforms to an NTRU cryptosystem," and, "the public-key obtaining subunit obtains a public-key polynomial generated according to a key-generation algorithm of

NTRU cryptosystem, as the public key," and, "the public-key encryption subunit generates a seed-value polynomial from the seed value, generates a blind-value polynomial from the blind value, and encrypts the seed-value polynomial according to an encryption algorithm of the NTRU cryptosystem, using the public-key polynomial as a key, and using the blind-value polynomial to randomize the seed-value polynomial, to generate an encryption seed-value polynomial as the encryption seed value," which is equivalent to Claims 10 & 12 of Application No. 10/725102.

Claims 14, 22, 28, & 36:

- Claim 13 of Application No. 10/725208 discloses, "the different computation algorithm is bitwise exclusive-or, and the second encryption subunit performs the bitwise exclusive-or on the verification value and the seed value, to generate the second cipher text," which is equivalent to Claims 14, 22, 28, & 36 of Application No. 10/725102.

Claims 15 & 29:

- Claim 12 of Application No. 10/725208 discloses, "the different computation algorithm is a symmetric key encryption algorithm, and the second encryption subunit performs the symmetric key encryption algorithm on the seed value using the verification value as a key, to generate the second cipher text," which is equivalent to Claims 15 & 29 of Application No. 10/725102.

Claims 16 & 30:

- Claim 14 of Application No. 10/725208 discloses, "the different computation algorithm is addition, and the second encryption subunit performs the addition on the verification

value and the seed value, to generate the second cipher text," which is equivalent to Claims 16 & 30 of Application No. 10/725102.

Claims 17 & 31:

- Claim 15 of Application No. 10/725208 discloses, "the different computation algorithm is multiplication, and the second encryption subunit performs the multiplication on the verification value and the seed value, to generate the second cipher text," which is equivalent to Claims 17 & 31 of Application No. 10/725102.

Claims 19, 20, & 21:

- Claim 10 of Application No. 10/725208 discloses, "the encryption unit generates the encryption information that includes the first cipher text and the second cipher text," which is equivalent to Claims 19, 20, & 21 of Application No. 10/725102.

Claim 23:

- Claim 22 of Application No. 10/725208 discloses equivalent elements as Claim 23 of Application No. 10/725102.

Claim 24:

- Claim 24 of Application No. 10/725102 discloses a shared-key recovery apparatus comprising equivalent elements as Claim 21 of Application No. 10/725208. The features disclosed in Claim 24 of Application No. 10/725102 as, "a first decryption unit operable to decrypt the first encryption information, to generate a first decryption verification value; a second decryption unit operable to decrypt the second encryption information based on the first decryption verification value, to generate a decryption seed value," are

equivalent to, "a decryption unit operable to decrypt the encryption information, to generate a decryption seed value," as disclosed by Application No. 10/725208.

Claim 25:

- Claim 22 of Application No. 10/725208 discloses, "the shared-key generation apparatus performs a one-way function on the seed value to generate a functional value, generates the blind value and the shared key from the functional value, obtains a public key, performs a public-key encryption algorithm on the seed value using the public key and the blind value, to generate an encryption seed value as the encryption information, and transmits the encryption seed value," and, "a secret-key obtaining subunit operable to obtain a secret key that corresponds to the public key; and a public-key decryption subunit operable to perform, on the received encryption seed value, a public-key decryption algorithm that corresponds to the public-key encryption algorithm, using the obtained secret key, to generate the decryption seed value," which is equivalent to Claim 25 of Application No. 10/725102.

Claim 26:

- Claims 23 & 27 of Application No. 10/725208 disclose elements equivalent to Claim 26 of Application No. 10/725102.

Claim 27:

- Claim 25 of Application No. 10/725208 discloses elements equivalent to Claim 27 of Application No. 10/725102.

Claim 37:

- Claim 22 of Application No. 10/725208 discloses, "the shared-key generation apparatus performs a one-way function on the seed value to generate a functional value, generates the blind value and the shared key from the functional value, obtains a public key, performs a public-key encryption algorithm on the seed value using the public key and the blind value, to generate an encryption seed value as the encryption information, and transmits the encryption seed value," and, "the shared-key generating unit performs the one-way function on the decryption seed value to generate a decryption functional value, and generates the decryption blind value and the decryption shared key from the decryption functional value," which is equivalent to Claim 37 of Application No. 10/725102.

Claim 40:

- Claim 28 of Application No. 10/725208 discloses, "the shared-key generation apparatus performs a one-way function on the seed value to generate a functional value, generates a verification value, the blind value, and the shared key from the functional value, obtains a public key, performs a public-key encryption algorithm on the verification value using the public key and the blind value to generate a first cipher text, performs, based on the verification value, a computation algorithm different from the public-key encryption algorithm on the seed value, to generate a second cipher text, generates the encryption information that includes the first cipher text and the second cipher text, and transmits the encryption information," which is equivalent to Claim 40 of Application No. 10/725102.

Claim 41:

- Claim 24 of Application No. 10/725208 discloses, "the shared-key generation apparatus obtains a public key, generates a blind value, performs a public-key encryption algorithm on the seed value using the public key and the blind value to generate a public-key cipher text, performs a second one-way function on at least one of the seed value, the blind value, and the shared key to generate a second functional value, generates the encryption information that includes the public-key cipher text and the second functional value, and transmits the encryption information," which is equivalent to the disclosure of Claim 41 of Application No. 10/725102, "the shared-key generation apparatus obtains a public key, performs a public-key encryption algorithm on the verification value, using the public key and the blind value, to generate the first encryption information."
- Claim 10 of Application No. 10/725208 discloses, "a public-key obtaining subunit operable to obtain the public key," which is equivalent to the disclosure of Claim 41 of Application No. 10/725102, "a public-key obtaining subunit operable to obtain the public key."
- Claim 21 of Application No. 10/725208 discloses, "a re-encryption unit operable to encrypt the decryption seed value based on the decryption blind value, to generate re-encryption information; a judging unit operable to judge, based on the encryption information and there-encryption information, whether the decryption shared key should be outputted," which is equivalent to the disclosure of Claim 41 of Application No. 10/725102, "a re-encryption subunit operable to perform the public-key encryption algorithm on one of the first decryption verification value and the second decryption

verification value, using the public key and the decryption blind value, to generate re-encryption information; and a judging subunit operable to judge, based on the first encryption information and the re-encryption information, whether the decryption shared key should be outputted or not."

Claims 42 & 44:

- Claim 29 of Application No. 10/725208 discloses, "the judging unit judges whether the encryption verification-value polynomial as the first cipher text is identical to the re-encryption verification-value polynomial as the re-encryption information," which is equivalent to Claims 42 & 44 of Application No. 10/725102.

Claim 43:

- Claim 29 of Application No. 10/725208 discloses, "the public-key encryption algorithm and the public-key decryption algorithm conform to an NTRU cryptosystem," and, "the shared-key generation apparatus obtains a public-key polynomial generated according to a key-generation algorithm of the NTRU cryptosystem, as the public key, generates a verification-value polynomial from the verification value, generates a blind-value polynomial from the blind value, encrypts the verification-value polynomial according to an encryption algorithm of the NTRU cryptosystem, using the public-key polynomial as a key, and using the blind-value polynomial to randomize the verification-value polynomial, to generate an encryption verification-value polynomial as the first cipher text, generates the encryption information that includes the encryption verification-value polynomial as the first cipher text and the second cipher text, and transmits the encryption information," and, "the public-key obtaining subunit obtains the public-key

polynomial," and, "the re-encryption subunit generates a decryption verification-value polynomial from the decryption verification value, generates a blind-value polynomial from the decryption blind value, and encrypts the decryption verification-value polynomial according to the encryption algorithm of the NTRU cryptosystem, using the public-key polynomial as a key, and using the blind-value polynomial to randomize the decryption verification-value polynomial, to generate a re-encryption verification-value polynomial as the re-encryption information," which is equivalent to Claim 43 of Application No. 10/725102.

Claim 45:

- Claim 37 of Application No. 10/725208 discloses, "the shared-key generation apparatus further obtains a content, encrypts the obtained content using the shared key to generate an encrypted content, and transmits the encrypted content, and the shared-key recovery apparatus further includes: a content receiving unit operable to receive the encrypted content; a decryption unit operable to decrypt the received encrypted content using the outputted decryption shared key, to generate a decrypted content; and a playback unit operable to playback the decrypted content," which is equivalent to Claim 45 of Application No. 10/725102.

Claim 46:

- Claim 38 of Application No. 10/725208 discloses, "a seed-value generating step of generating a seed value; a shared-key generating step of generating a blind value and a shared key, from the seed value; an encryption step of encrypting the seed value based on the blind value, to generate encryption information; and a transmitting step of

transmitting the encryption information," which is equivalent to Claim 46 of Application No. 10/725102.

Claim 47:

- Claim 39 of Application No. 10/725208 discloses, "a seed-value generating step of generating a seed value; a shared-key generating step of generating a blind value and a shared key, from the seed value; an encryption step of encrypting the seed value based on the blind value, to generate encryption information; and a transmitting step of transmitting the encryption information," which is equivalent to Claim 47 of Application No. 10/725102.

Claim 48:

- Claim 40 of Application No. 10/725208 discloses, "the shared-key generating program is recorded in a computer-readable recording medium," which is equivalent to Claim 48 of Application No. 10/725102.

Claim 49:

- Claim 41 of Application No. 10/725208 discloses, "a receiving step of receiving the encryption information," and, "a decryption step of decrypting the encryption information, to generate a decryption seed value," and, "a shared-key generating step of generating a decryption blind value and a decryption shared key, using the decryption seed value and according to a same shared-key generating method used in the shared-key generation apparatus," and, "a judging step of judging, based on the encryption information and there-encryption information, whether the decryption shared key should be outputted," and, "an outputting step, when the judging unit has judged affirmatively,

of outputting the decryption shared key," which is equivalent to Claim 49 of Application No. 10/725102.

Claim 50:

- Claim 42 of Application No. 10/725208 discloses, "a receiving step of receiving the encryption information," and, "a decryption step of decrypting the encryption information, to generate a decryption seed value," and, "a shared- key generating step of generating a decryption blind value and a decryption shared key, using the decryption seed value and according to a same shared-key generating method used in the shared-key generation apparatus," and, "a judging step of judging, based on the encryption information and there-encryption information, whether the decryption shared key should be outputted," and, "an outputting step, when the judging unit has judged affirmatively, of outputting the decryption shared key," which is equivalent to Claim 50 of Application No. 10/725102.

Claim 51:

- Claim 43 of Application No. 10/725208 discloses, "The shared-key recovery program is recorded in a computer-readable recording medium," which is equivalent to Claim 51 of Application No. 10/725102.

Claim Rejections - 35 USC § 101

2. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 39 & 42 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

- Claim 39: The applicant discloses, "a shared-key generating program used in a shared-key generation apparatus that notifies a destination apparatus about a shared key, in secrecy," however, a program is non-statutory subject matter as in accordance to 35 U.S.C. 101.
- Claim 42: The applicant discloses, "a share-key recovery program used in a shared-key recovery apparatus that receives a shared key from a shared-key generation apparatus in secrecy," however, a program is non-statutory subject matter as in accordance to 35 U.S.C. 101.

Examiner's Note

The examiner notes that Claims 39 and 42 of this application will be interpreted as being computer programs with computer executable/readable instructions stored on a computer readable medium for the rejections below.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1-12, 16-29, 34-39, 41, & 42 are rejected under 35 U.S.C. 102(b) as being anticipated by Hoffstein (WO-9808323-A1).

Claim 1:

Hoffstein discloses a key agreement system as in Claim 1 of the applicant comprising,

- "the key creator, call him Dan..." and the equations or formulas which disclose the system functions of, "a seed-value generating unit operable to generate a seed value; a first shared-key generating unit operable to generate a blind value and a shared key, from the seed value" [pages 13-15].
- "the encoder, call her Cathy..." and the equations or formulas which disclose the system functions of, "an encryption unit operable to encrypt the seed value based on the blind value, to generate encryption information" [page 16].
- "Communication is via transceiver" (i.e. "a transmitting unit operable to transmit the encryption information") [page 8 lines 22-24].
- Fig 5 (i.e. "a receiving unit operable to receive the encryption information") [Fig 5 Box# 530].

- "Dan..." and the equations or formulas disclosed by Hoffstein on pages 17-18 (i.e. "a decryption unit operable to decrypt the encryption information, to generate a decryption seed value") [pages 17-18].
- "Dan..." and the equations or formulas disclosed by Hoffstein on pages 17-18 (i.e. "a second shared-key generating unit operable to generate a decryption blind value and a decryption shared key, using the decryption seed value and according t o a same method as used in the first shared key generating unit ") [pages 17-18].
- The explanations accompanied by equations or formulas disclosed by Hoffstein on pages 19-20 (i.e. "a re-encryption unit operable to encrypt the decryption seed value based on the decryption blind value, to generate re-encryption information") [pages 19-20].
- Fig 6 ("i.e. a judging unit operable to judge, based on the encryption information and the re-encryption information, whether the decryption shared key should be outputted") [Fig 6 Box# 640].
- "The block 210 represents the generating of the public and private key information, and the 'publishing' of the public key" ("i.e. "an outputting unit operable, when the judging unit has judged affirmatively, to output the decryption shared key") [page 22 lines 7-9 & 12-23].

Claim 2:

Hoffstein discloses a key agreement system as in Claim 1 above further comprising,

- Fig 4 ("i.e. an obtaining unit operable to obtain a content") [Fig 4 Box# 420].
- "The encoding technique of an embodiment of the public key cryptosystem hereof uses a mixing system based on polynomial algebra and reduction modulo two numbers, p and q,

while the decoding technique uses an unmixing system whose validity depends on the elementary probability theory" (i.e. "an encryption unit operable to encrypt the obtained content using the shared key, to generate an encrypted content") [page 9].

- "Communication is via transceiver..." (i.e. "the transmitting unit further transmits the encrypted content") [page 8 lines 22-24].
- Fig 5 (i.e. "the receiving unit further receives the encrypted content") [Fig 5 Box# 530].
- "The decoding for this matrix example is described next..." (i.e. "a decryption unit operable to decrypt the received encrypted content using the decryption shared key, to generate a decrypted content") [page 20].
- "Finally Dan computes...to recover the original message m." (i.e. "an outputting unit operable to output the decrypted content" [page 20].

Claim 3:

Hoffstein discloses a shared-key generation apparatus used in the key agreement system as in Claim 1 above comprising,

- "the key creator, call him Dan..." and the equations or formulas which disclose the system functions of, (i.e. "a seed-value generating unit operable to generate a seed value," and, "a shared-key generating unit operable to generate a blind value and a shared key, from the seed value") [pages 13-15].
- "the encoder, call her Cathy..." and the equations or formulas which disclose the system functions of, "an encryption unit operable to encrypt the seed value based on the blind value, to generate encryption information" [pages 15-16].

- "Communication is via transceiver" (i.e. "a transmitting unit operable to transmit the encryption information") [page 8 lines 22-24].

Claim 4:

Hoffstein discloses a shared-key generation apparatus used in the key agreement system as in Claim 3 above further comprising,

- "She uses this randomly chosen polynomial Θ, Dan's public key h, and her plaintext message m to create the encoded message e using the formula" (i.e. "the shared-key generating unit performs a one-way function on the seed value to generate a functional value, and generates the blind value and the shared key from the functional value") [pages 16-17].
- "The public key information can be published; that is, made available to any member of the public or to any desired group..." (i.e. "a public-key obtaining subunit operable to obtain a public key") [page 22 lines 12-23].
- "The block 220 represents the routine that can be used by the message sender to encode the plaintext message using the public key of the intended message recipient." (i.e. "a public-key encryption subunit operable to perform a public-key encryption algorithm on the seed value, using the public key and the blind value, to generate an encryption seed value as the encryption information") [page 22 lines 24-27 & page 23 lines 1-4].

Claim 5:

Hoffstein discloses a shared-key generation apparatus used in the key agreement system as in Claim 4 above further comprising,

- "1.2 Key Creation. To create an NTRU key," (i.e. "the public-key encryption algorithm conforms to an NTRU cryptosystem") [page 31].
- "Dan randomly chooses...The polynomial f must satisfy the additional requirement... Dan next computes the quantities... Dan's public key is the list of polynomials... Dan's private key is the single polynomial f..." (i.e. "the public-key obtaining subunit obtains a public-key polynomial generated according to a key-generation algorithm of the NTRU cryptosystem, as the public key,") [page 31].
- "1.2 Key Creation...1.3 Encoding..." (i.e. "the public-key encryption subunit generates a seed-value polynomial from the seed value, generates a blind-value polynomial from the blind value, and encrypts the seed-value polynomial according to an encryption algorithm of the NTRU cryptosystem, using the public-key polynomial as a key, and using the blind-value polynomial to randomize the seed-value polynomial, to generate an encryption seed-value polynomial as the encryption seed value") [page 31].
- "Communication is via transceiver" (i.e. "the transmitting unit transmits the encryption seed-value polynomial as the encryption seed value") [page 8 lines 22-24].

Claim 6:

Hoffstein discloses a shared-key generation apparatus used in the key agreement system as in Claim 3 above further comprising,

- "The public key information can be published; that is, made available to any member of the public or to any desired group..." (i.e. "a public-key obtaining subunit operable to obtain a public key") [page 22 lines 12-23].
- "The block 220 represents the routine that can be used by the message sender to encode the plaintext message using the public key of the intended message recipient." (i.e. "a public-key encryption subunit operable to generate a blind value, perform the public-key encryption algorithm on the seed value using the public key and the blind value, to generate a public-key cipher text") [page 22 lines 24-27 & page 23 lines 1-4].
- The explanations accompanied by equations or formulas disclosed by Hoffstein on pages 13-15 (i.e. "a function subunit operable to perform a second one-way function on at least one of the seed value, the blind value, and the shared key, to generate a second functional value, and the encryption unit generates the encryption information that includes the public-key cipher text and the second functional value" [pages 13-15].

Claim 7:

Hoffstein discloses a shared-key generation apparatus used in the key agreement system as in Claim 6 above further comprising,

- "1.2 Key Creation...1.3 Encoding" (i.e. "the shared-key generating unit performs a one-way function on the seed value, to generate a functional value, and generates the blind value and the shared key from the functional value") [page 31].

Claim 8:

Hoffstein discloses a shared-key generation apparatus used in the key agreement system as in Claim 6 above further comprising,

- The explanations accompanied by equations or formulas disclosed by Hoffstein on pages 13-15 (i.e. "the shared-key generating unit performs a first one-way function on the seed value, to generate a first functional value, and generates the shared key from the first functional value, instead of generating the blind value and the shared key" [pages 13-15].

Claim 9:

Hoffstein discloses a shared-key generation apparatus used in the key agreement system as in Claim 6 above further comprising,

- "1.2 Key Creation...1.3 Encoding" (i.e. "the public-key encryption algorithm conforms to an NTRU cryptosystem, the public-key obtaining subunit obtains a public-key polynomial generated according to a key-generation algorithm of the NTRU cryptosystem, as the public key, the public-key encryption subunit generates a seed-value polynomial from the seed value, generates a blind-value polynomial from the blind value, encrypts the seed-value polynomial according to an encryption algorithm of the NTRU cryptosystem, using the public-key polynomial as a key, and using the blind-value polynomial to randomize the seed-value polynomial, to generate an encryption seed-value polynomial as the public-key cipher text,") [page 31].
- The explanations accompanied by equations or formulas disclosed by Hoffstein on pages 13-15 (i.e. "the encryption unit generates the encryption information that includes the

encryption seed value polynomial as the public-key cipher text and the second functional value" [pages 13-15].

Claim 10:

Hoffstein discloses a shared-key generation apparatus used in the key agreement system as in Claim 3 above further comprising,

- The explanations accompanied by equations or formulas disclosed by Hoffstein on pages 16-17 (i.e. "the shared-key generating unit performs a one-way function on the seed value, to generate a functional value, and -generates a verification value, the blind value, and the shared key, from the functional value," and, "a second encryption subunit operable to perform, on the seed value, a computation algorithm different from the public-key encryption algorithm, to generate a second cipher text, and the encryption unit generates the encryption information that includes the first cipher text and the second cipher text" [pages 16-17].
- "The public key information can be published; that is, made available to any member of the public or to any desired group..." (i.e. "a public-key obtaining subunit operable to obtain the public key") [page 22 lines 12-23].
- "The block 220 represents the routine that can be used by the message sender to encode the plaintext message using the public key of the intended message recipient." (i.e. "a first encryption subunit operable to perform a public-key encryption algorithm on the verification value, using the public key and the blind value, to generate a first cipher text") [page 22 lines 24-27 & page 23 lines 1-4].

Claim 11:

Hoffstein discloses a shared-key generation apparatus used in the key agreement system as in Claim 10 above further comprising,

- "1.2 Key Creation...1.3 Encoding" (i.e. "the public-key encryption algorithm conforms to an NTRU cryptosystem, The public-key obtaining subunit obtains a public-key polynomial generated according to a key-generation algorithm of the NTRU cryptosystem, as the public key, the first encryption subunit generates a verification-value polynomial from the verification value, generates a blind-value polynomial from the blind value, and encrypts the verification-value polynomial according to an encryption algorithm of the NTRU cryptosystem, using the public- key polynomial as a key, and using the blind-value polynomial to randomize the verification-value polynomial, to generate an encryption verification-value polynomial as the first cipher text,") [page 31].
- The explanations accompanied by equations or formulas disclosed by Hoffstein on pages 13-15 (i.e. "the encryption unit generates the encryption information that includes the encryption verification-value polynomial as the first cipher text and the second cipher text" [pages 13-15].

Claim 12:

Hoffstein discloses a shared-key generation apparatus used in the key agreement system as in Claim 11 above further comprising,

- The explanations accompanied by equations or formulas disclosed by Hoffstein on pages 16-17 (i.e. "the different computation algorithm is a symmetric key encryption algorithm, and the second encryption subunit performs the symmetric key encryption algorithm on

the seed value using the verification value as a key, to generate the second cipher text") [pages 16-17].

Claim 16:

Hoffstein discloses a shared-key generation apparatus used in the key agreement system as in Claim 3 above further comprising,

- "...choose integer parameters N, K, p, and q... " and the referenced equations or formulas which disclose the system functions of, (i.e. "the seed-value generating unit generates a random number, as the seed value") [pages 13-14].

Claim 17:

Hoffstein discloses a shared-key generation apparatus used in the key agreement system as in Claim 3 above further comprising,

- The explanations accompanied by equations or formulas disclosed by Hoffstein on pages 16-17 (i.e. "the shared-key generating unit performs a one-way function on the seed value, to generate a functional value, and generates the blind value and the shared key from the functional value") [pages 16-17].

Claim 18:

Hoffstein discloses a shared-key generation apparatus used in the key agreement system as in Claim 17 above further comprising,

- The explanations accompanied by equations or formulas disclosed by Hoffstein on pages 16-17 (i.e. "the one-way function is a hash function , and the shared-key generating unit performs the hash function on the seed value") [pages 16-17].

Claim 19:

Hoffstein discloses a shared-key generation apparatus used in the key agreement system as in Claim 17 above further comprising,

- "1.2 Key Creation...1.3 Encoding" (i.e. "the shared-key generating unit generates the blind value by setting a part of the functional value as the blind value, and generates the shared key by setting another part of the functional value as the shared key") [page 31].

Claim 20:

Hoffstein discloses a shared-key generation apparatus used in the key agreement system as in Claim 3 above further comprising,

- Fig 4 (i.e. "an obtaining unit operable to obtain a content") [Fig 4 Box# 420].
- "The encoding technique of an embodiment of the public key cryptosystem hereof uses a mixing system based on polynomial algebra and reduction modulo two numbers, p and q, while the decoding technique uses an unmixing system whose validity depends on the elementary probability theory" (i.e. "an encryption unit operable to encrypt the obtained content using the shared key, to generate an encrypted content") [page 9].
- "Communication is via transceiver" (i.e. "the transmitting unit further transmits the encrypted content") [page 8 lines 22-24].

Claim 21:

Hoffstein discloses a shared-key recovery apparatus used in the key agreement system as in Claim 1 above comprising,

- Fig 5 (i.e. "a receiving unit operable to receive the encryption information") [Fig 5 Box# 530].

- "Dan..." and the equations or formulas disclosed by Hoffstein on pages 16-17 (i.e. "a decryption unit operable to decrypt the encryption information, to generate a decryption seed value") [pages 17-18].
- "the key creator, call him Dan..." and the equations or formulas which disclose the system functions of, (i.e. "a shared-key generating unit operable to generate a decryption blind value and a decryption shared key, using the decryption seed value and according to a same shared-key generating method used in the shared-key generation apparatus") [pages 14-15].
- The explanations accompanied by equations or formulas disclosed by Hoffstein on pages 16-17 (i.e. "a re-encryption unit operable to encrypt the decryption seed value based on the decryption blind value, to generate re-encryption information") [pages 16-17].
- Fig 6 (i.e. "a judging subunit operable to judge, based on the encryption information and the re-encryption information, whether the decryption shared key should be outputted") [Fig 6 Box# 640].
- "The block 210 represents the generating of the public and private key information, and the 'publishing' of the public key" ("i.e. "an outputting unit operable, when the judging unit has judged affirmatively, to output the decryption shared key") [page 22 lines 7-9 & 12-23].

Claim 22:

Hoffstein discloses a shared-key recovery apparatus used in the key agreement system as in Claim 21 above further comprising,

- "1.2 Key Creation...1.3 Encoding" (i.e. "the shared-key generation apparatus performs a one-way function on the seed value to generate a functional value, generates the blind value and the shared key from the functional value, obtains a public key, performs a public-key encryption algorithm on the seed value using the public key and the blind value, to generate an encryption seed value as the encryption information, and transmits the encryption seed value," and, "a public-key decryption subunit operable to perform, on the received encryption seed value, a public-key decryption algorithm that corresponds to the public-key encryption algorithm, using the obtained secret key, to generate the decryption seed value") [page 31].
- Fig 5 (i.e. "the receiving unit receives the encryption seed value as the encryption information") [Fig 5 Box# 530].
- "The public key information can be published; that is, made available to any member of the public or to any desired group..." (i.e. "a secret-key obtaining subunit operable to obtain a secret key that corresponds to the public key") [page 22 lines 12-23].
- The explanations accompanied by equations or formulas disclosed by Hoffstein on pages 16-17 (i.e. "the shared-key generating unit performs the one-way function on the decryption seed value to generate a decryption functional value, and generates the decryption blind value and the decryption shared key from the decryption functional

value, the re-encryption unit includes: a public-key obtaining subunit operable to obtain the public key") [pages 16-17].

- "The decoding for this matrix example is described next..." (i.e. "a re-encryption subunit operable to perform the public-key encryption algorithm on the decryption seed value using the public key and the decryption blind value, to generate a re-encryption seed value as the re-encryption information, and the judging unit judges whether the encryption seed value is identical to the re-encryption seed value, and when judging affirmatively, determines that the decryption shared key should be outputted") [page 20].

Claim 23:

Hoffstein discloses a shared-key recovery apparatus used in the key agreement system as in Claim 22 above further comprising,

- "1.2 Key Creation...1.3 Encoding...1.4 Decoding..." (i.e. "the public-key encryption algorithm and the public key decryption algorithm conform to an NTRU cryptosystem, the shared-key generation apparatus obtains a public-key polynomial generated according to a key-generation algorithm of the NTRU cryptosystem, as the public key, generates a seed-value polynomial from the seed value, generates a blind-value polynomial from the blind value, encrypts the seed-value polynomial according to an encryption algorithm of the NTRU cryptosystem, using the public key polynomial as a key, and using the blind-value polynomial to randomize the seed-value polynomial, to generate an encryption seed-value polynomial as the encryption seed value, and transmits the encryption seed-value polynomial as the encryption seed value, the receiving unit receives the encryption seed-value polynomial as the encryption seed value, the secret-key obtaining subunit

obtains a secret-key polynomial generated according to the key-generation algorithm of the NTRU cryptosystem, as the secret key, the public-key decryption subunit decrypts the received encryption seed-value polynomial according to a decryption algorithm of the NTRU cryptosystem and using the obtained secret-key polynomial as a key, to generate a decryption seed-value polynomial, and generates the decryption seed value from the decryption seed-value polynomial") [page 31].

- "The public key information can be published; that is, made available to any member of the public or to any desired group..." (i.e. "the public-key obtaining subunit obtains the public-key polynomial as the public key") [page 22 lines 12-23].
- "The decoding for this matrix example is described next..." (i.e. "the re-encryption subunit generates a seed-value polynomial from the decryption seed value, generates a blind-value polynomial from the decryption blind value, and encrypts the seed-value polynomial according to the encryption algorithm of the NTRU cryptosystem, using the public-key polynomial as a key, and using the blind-value polynomial to randomize the seed-value polynomial, to generate a re-encryption seed-value polynomial, and the judging unit judges whether the encryption seed value polynomial is identical to the re-encryption seed-value polynomial") [page 20].

Claim 24:

Hoffstein discloses a shared-key recovery apparatus used in the key agreement system as in Claim 21 above further comprising,

- The explanations accompanied by equations or formulas disclosed by Hoffstein on pages 16-17 (i.e. "the shared-key generation apparatus obtains a public key, generates a blind

value, performs a public-key encryption algorithm on the seed value using the public key and the blind value to generate a public-key cipher text, performs a second one-way function on at least one of the seed value, the blind value, and the shared key to generate a second functional value, generates the encryption information that includes the public-key cipher text and the second functional value, and transmits the encryption information," and, "a public-key decryption subunit operable to perform, on the public-key cipher text included in the received encryption information, a public-key decryption algorithm that corresponds to the public-key encryption algorithm, to generate a decryption seed value; and a function subunit operable to perform the second one-way function on at least one of the decryption seed value, the decryption blind value, and the decryption shared key, to generate a decryption second functional value") [pages 16-17].

- "1.2 Key Creation...1.3 Encoding...1.4 Decoding..." (i.e. "the receiving unit receives the encryption information that includes the public-key cipher text and the second functional value, the decryption unit includes: a secret-key obtaining subunit operable to obtain a secret key that corresponds to the public key") [page 31].
- "The decoding for this matrix example is described next..." (i.e. "the judging unit judges whether the second functional value included in the received encryption information is identical to the decryption second functional value instead of performing judging based on the encryption information and the re-encryption information, and when judging affirmatively, determines that the decryption shared key should be outputted") [page 20].

Claim 25:

Hoffstein discloses a shared-key recovery apparatus used in the key agreement system as in Claim 24 above further comprising,

- The explanations accompanied by equations or formulas disclosed by Hoffstein on pages 16-17 (i.e. "the shared-key generation apparatus performs a one-way function on the seed value to generate a functional value, and generates the blind value and the shared key from the functional value, and the shared-key generating unit performs the first one-way function on the decryption seed value to generate a decryption functional value, and generates the decryption blind value and the decryption shared key from the decryption functional value") [pages 16-17].

Claim 26:

Hoffstein discloses a shared-key recovery apparatus used in the key agreement system as in Claim 24 above further comprising,

- The explanations accompanied by equations or formulas disclosed by Hoffstein on pages 16-17 (i.e. "the shared-key generation apparatus performs a first one-way function on the seed value to generate a first functional value, and generates the shared key from the first functional value, instead of generating the blind value and the shared key, and the shared-key generating unit performs the first one-way function on the decryption seed value to generate a decryption functional value, and generates the decryption shared key from the decryption functional value, instead of generating the decryption blind value and the decryption shared key") [pages 16-17].

Claim 27:

Hoffstein discloses a shared-key recovery apparatus used in the key agreement system as in Claim 24 above further comprising,

- "1.2 Key Creation...1.3 Encoding...1.4 Decoding..." (i.e. "the public-key encryption algorithm and the public-key decryption algorithm conform to an NTRU cryptosystem, the shared-key generation apparatus obtains a public-key polynomial generated according to a key-generation algorithm of the NTRU cryptosystem, as the public key, generates a seed-value polynomial from the seed value, generates a blind-value polynomial from the blind value, encrypts the seed-value polynomial according to an encryption algorithm of the NTRU cryptosystem using the public key polynomial as a key and using the blind-value polynomial to randomize the seed-value polynomial, to generate an encryption seed-value polynomial as the public-key cipher text, and generates the encryption information that includes the encryption seed-value polynomial as the public-key cipher text and the second functional value, the secret-key obtaining subunit obtains a secret-key polynomial generated according to the key-generation algorithm of the NTRU cryptosystem, as the secret key, and the public-key decryption subunit generates a public-key cipher-text polynomial from the public-key cipher text, decrypts the public-key cipher-text polynomial according to a decryption algorithm of the NTRU cryptosystem using the secret-key polynomial as a key to generate a decryption seed-value polynomial, and generates the decryption seed value from the decryption seed-value polynomial") [page 31].

Claim 28:

Hoffstein discloses a shared-key recovery apparatus used in the key agreement system as in Claim 21 above further comprising,

- "1.2 Key Creation...1.3 Encoding...1.4 Decoding..." (i.e. "the shared-key generation apparatus performs a one-way function on the seed value to generate a functional value, generates a verification value, the blind value, and the shared key from the functional value, obtains a public key, performs a public-key encryption algorithm on the verification value using the public key and the blind value to generate a first cipher text, performs, based on the verification value, a computation algorithm different from the public-key encryption algorithm on the seed value, to generate a second cipher text, generates the encryption information that includes the first cipher text and the second cipher text, and transmits t h e encryption information, the receiving unit receives the encryption information that includes the first cipher text and the second cipher text") [page 31].
- The explanations accompanied by equations or formulas disclosed by Hoffstein on pages 16-17 (i.e. "a secret-key obtaining subunit operable to obtain a secret key that corresponds to the public key; a public-key decryption subunit operable to perform, on the first cipher text included in the received encryption information, a public-key decryption algorithm that corresponds to the public-key encryption algorithm, to generate a decryption verification value; and a computation decryption subunit operable to perform, on the second cipher text included in the received encryption information, a computation algorithm for performing an inverse computation of the different

computation algorithm, to generate a decryption seed value, the shared-key generating unit performs the one-way function on the decryption seed value to generate a decryption functional value, and generates a decryption verification value, the decryption blind value, and the decryption shared key, from the decryption functional value, the re-encryption unit includes: a public-key obtaining subunit operable to obtain the public key") [pages 16-17].

- "The decoding for this matrix example is described next..." (i.e. "a re-encryption subunit operable to perform, on the decryption verification value, the public-key encryption algorithm using the public key and the decryption blind value, to generate the re encryption information, and the judging unit judges whether the first cipher text included in the encryption information is identical to the re-encryption information, and when judging affirmatively, determines that the decryption shared key should be outputted") [page 20].

Claim 29:

Hoffstein discloses a shared-key recovery apparatus used in the key agreement system as in Claim 28 above further comprising,

- "1.2 Key Creation...1.3 Encoding...1.4 Decoding..." (i.e. "the public-key encryption algorithm and the public-key decryption algorithm conform to an NTRU cryptosystem, the shared-key generation apparatus obtains a public-key polynomial generated according to a key-generation algorithm of the NTRU cryptosystem, as the public key, generates a verification-value polynomial from the verification value, generates a blind-value polynomial from the blind value, encrypts the verification-value polynomial according to

an encryption algorithm of the NTRU cryptosystem, using the public-key polynomial as a key, and using the blind-value polynomial to randomize the verification-value polynomial, to generate an encryption verification-value polynomial as the first cipher text, generates the encryption information that includes the encryption verification-value polynomial as the first cipher text and the second cipher text, and transmits the encryption information, the receiving unit receives the encryption information that includes the encryption verification-value polynomial and the second cipher text, the secret-key obtaining subunit obtains a secret-key polynomial generated according to the key-generation algorithm of the NTRU cryptosystem, as the secret key") [page 31].

- The explanations accompanied by equations or formulas disclosed by Hoffstein on pages 16-17 (i.e. "the public-key decryption subunit generates a first cipher-text polynomial from the first cipher text, decrypts the first cipher-text polynomial according to a decryption algorithm of the NTRU cryptosystem using the secret-key polynomial as a key, to generate a decryption verification polynomial, and generates the decryption verification value from the decryption verification-value polynomial, the public-key obtaining subunit obtains the public-key polynomial, the re-encryption subunit generates a decryption verification-value polynomial from the decryption verification value, generates a blind-value polynomial from the decryption blind value, and encrypts the decryption verification-value polynomial according to the encryption algorithm of the NTRU cryptosystem, using the public-key polynomial as a key, and using the blind-value polynomial to randomize the decryption verification-value polynomial, to generate a re-

encryption verification-value polynomial as the re-encryption information") [pages 16-17].

- "The decoding for this matrix example is described next..." (i.e. "the judging unit judges whether the encryption verification-value polynomial as the first cipher text is identical to the re-encryption verification-value polynomial as the re-encryption information") [page 20].

Claim 34:

Hoffstein discloses a shared-key recovery apparatus used in the key agreement system as in Claim 21 above further comprising,

- The explanations accompanied by equations or formulas disclosed by Hoffstein on pages 16-17 (i.e. "the shared-key generating unit performs a one-way function on the decryption seed value to generate a functional value, and generates the decryption blind value and the decryption shared key from the functional value") [pages 16-17].

Claim 35:

Hoffstein discloses a shared-key recovery apparatus used in the key agreement system as in Claim 34 above further comprising,

- The explanations accompanied by equations or formulas disclosed by Hoffstein on pages 16-17 (i.e. "the one-way function is a hash function, and the shared-key generating unit performs the hash function on the decryption seed value") [pages 16-17].

Claim 36:

Hoffstein discloses a shared-key recovery apparatus used in the key agreement system as in Claim 34 above further comprising,

- The explanations accompanied by equations or formulas disclosed by Hoffstein on pages 16-17 (i.e. "the shared-key generating unit generates the decryption blind value by setting a part of the functional value as the decryption blind value, and generates the decryption shared key by setting another part of the functional value as the decryption shared key") [pages 16-17].

Claim 37:

Hoffstein discloses a shared-key recovery apparatus used in the key agreement system as in Claim 21 above further comprising,

- The explanations accompanied by equations or formulas disclosed by Hoffstein on pages 16-17 (i.e. "the shared-key generation apparatus further obtains a content, encrypts the obtained content using the shared key to generate an encrypted content, and transmits the encrypted content") [pages 16-17].
- Fig 5 (i.e. "a content receiving unit operable to receive the encrypted content") [Fig 5 Box# 530].
- "The decoding for this matrix example is described next..." (i.e. "a decryption unit operable to decrypt the received encrypted content using the outputted decryption shared key, to generate a decrypted content; and a playback unit operable to playback the decrypted content") [page 20].

Claim 38:

Hoffstein discloses a shared-key generating method used in the key agreement system as in Claim 1 above further comprising,

- The explanations accompanied by equations or formulas disclosed by Hoffstein on pages 13-15 (i.e. "a seed-value generating step of generating a seed value; a shared-key generating step of generating a blind value and a shared key, from the seed value" [pages 13-15].
- The explanations accompanied by equations or formulas disclosed by Hoffstein on pages 16-17 (i.e. "an encryption step of encrypting the seed value based on the blind value, to generate encryption information") [pages 16-17].
- "Communication is via transceiver" (i.e. "a transmitting step of transmitting the encryption information") [page 8 lines 22-24].

Claim 39:

Hoffstein discloses a shared-key generating program used in the key agreement system as in Claim 1 above further comprising,

- The explanations accompanied by equations or formulas disclosed by Hoffstein on pages 13-15 (i.e. "a seed-value generating step of generating a seed value; a shared-key generating step of generating a blind value and a shared key, from the seed value" [pages 13-15].
- The explanations accompanied by equations or formulas disclosed by Hoffstein on pages 16-17 (i.e. "an encryption step of encrypting the seed value based on the blind value, to generate encryption information") [pages 16-17].

- "Communication is via transceiver" (i.e. "a transmitting step of transmitting the encryption information") [page 8 lines 22-24].

Claim 41:

Hoffstein discloses a shared-key recovery method used in the key agreement system as in Claim 1 above further comprising,

- Fig 5 (i.e. "a receiving step of receiving the encryption information") [Fig 5 Box# 530].
- The explanations accompanied by equations or formulas disclosed by Hoffstein on pages 16-17 (i.e. "a decryption step of decrypting the encryption information, to generate a decryption seed value; a shared-key generating step of generating a decryption blind value and a decryption shared key, using the decryption seed value and according to a same shared-key generating method used in the shared-key generation apparatus") [pages 16-17].
- "The decoding for this matrix example is described next..." (i.e. "are-encryption step of encrypting the decryption seed value based on the decryption blind value, to generate re encryption information; a judging step of judging, based on the encryption information and there-encryption information, whether the decryption shared key should be outputted; and an outputting step, when the judging unit has judged affirmatively, of outputting the decryption shared key") [page 20].

Claim 42:

Hoffstein discloses a shared-key recovery program used in the key agreement system as in Claim 1 above further comprising,

- Fig 5 (i.e. "a receiving step of receiving the encryption information") [Fig 5 Box# 530].
- The explanations accompanied by equations or formulas disclosed by Hoffstein on pages 16-17 (i.e. "a decryption step of decrypting the encryption information, to generate a decryption seed value; a shared-key generating step of generating a decryption blind value and a decryption shared key, using the decryption seed value and according to a same shared-key generating method used in the shared-key generation apparatus") [pages 16-17].
- "The decoding for this matrix example is described next..." (i.e. "are-encryption step of encrypting the decryption seed value based on the decryption blind value, to generate re encryption information; a judging step of judging, based on the encryption information and there-encryption information, whether the decryption shared key should be outputted; and an outputting step, when the judging unit has judged affirmatively, of outputting the decryption shared key") [page 20].

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 13-15, 30-33, 40, & 43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hoffstein (WO-9808323-A1).

Claims 13-15, & 30-33:

- Hoffstein discloses a key agreement system as in Claim 1 above, but does not explicitly disclose, "the different computation algorithm is bitwise exclusive-or, and the second encryption subunit performs the bitwise exclusive-or on the verification value and the seed value, to generate the second cipher text," and, "the different computation algorithm is addition, and the second encryption subunit performs the addition on the verification value and the seed value, to generate the second cipher text," and, "the different computation algorithm is multiplication, and the second encryption subunit performs the multiplication on the verification value and the seed value, to generate the second cipher text," and, "the different computation algorithm is a symmetric key encryption algorithm, and the computation algorithm for performing the inverse computation is a corresponding symmetric key decryption algorithm, and the computation decryption subunit performs the symmetric key decryption algorithm on the second cipher text, using the decryption verification value as a key, to generate the decryption seed value," and, "the different computation algorithm and the computation algorithm for performing the inverse

computation are bitwise exclusive-or, and the computation decryption subunit performs the bitwise exclusive-or on the decryption verification value and the second cipher text, to generate the decryption seed value," and, "the different computation algorithm is addition and the computation algorithm for performing the inverse computation is subtraction, and the computation decryption subunit performs the subtraction on the decryption verification value and the second cipher text, to generate the decryption seed value," and, "the different calculation algorithm is multiplication and the computation algorithm for performing the inverse computation is division, and the computation decryption subunit performs the division on the decryption verification value and the second cipher text, to generate the decryption seed value." However, Hoffstein does disclose a plurality of algorithms, equations, and/or formulas showing examples of methods of calculations that can be performed to successfully enable encryption in the disclosed invention. Therefore, it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include the features disclosed by Hoffstein for the purposes of successfully enabling encryption in the invention.

Claims 40 & 43:

- Hoffstein discloses a key agreement system as in Claim 1 above, but does not explicitly disclose, "the shared-key generating program is recorded in a computer-readable recording medium," and "The shared-key recovery program is recorded in a computer-readable recording medium". However, Hoffstein does disclose, "it will be understood that the public or private keys can be stored on any suitable media, for example a 'smart card', which can be provided with a microprocessor capable of performing encoding

and/or decoding, so that encrypted messages can be communicated to and/or from the smart card." Therefore, it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include the features of Hoffstein for the purposes of storage and enabling the ability for the shared-key programs to be executed and processed by a microprocessor for performing the encoding/decoding (i.e. encryption/decryption) of messages.

Conclusion

1. The prior art made of record and not relied upon is considered pertinent to the applicant's disclosure.

a. Matyas (US-5953420-A)

2. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Examiner Oscar Louie whose telephone number is 571-270-1684. The examiner can normally be reached Monday through Thursday from 7:30 AM to 4:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Myhre, can be reached at 571-270-1065. The fax phone number for Formal or Official faxes to Technology Center 2100 is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private

PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

OAL
01/10/2007

James Myhre
Supervisory Patent Examiner